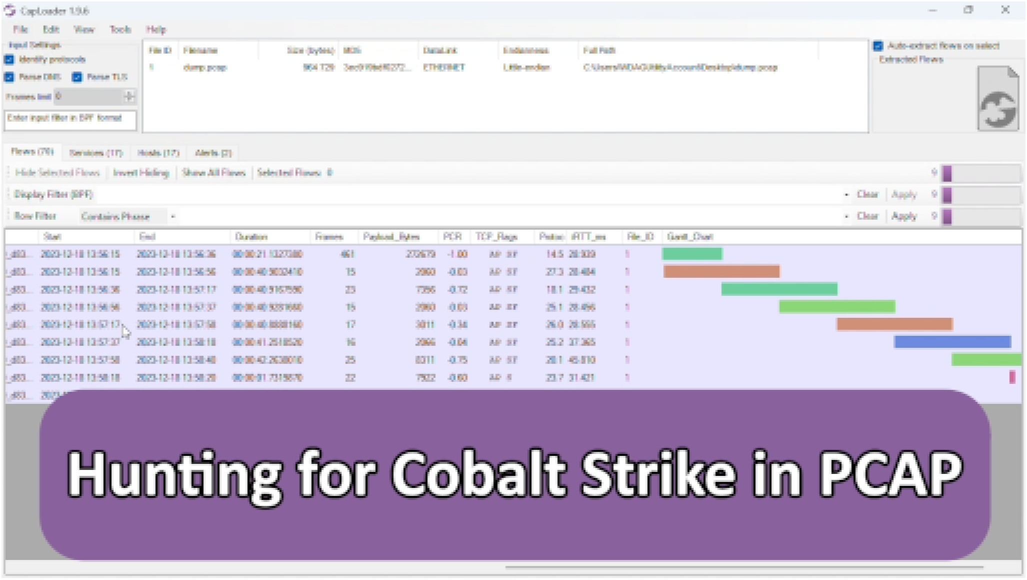
Hunting for Cobalt Strike in PCAP

netresec.com/

January 4, 2024



File ID	Filename	Size (bytes)	MD5	DataLink	Endianness	Full Path
1	dump.pcap	964 729	3ec9106e8f0272...	ETHERNET	Little-endian	C:\Users\WDAGUtilityAccount\Desktop\dump.pcap

	Start	End	Duration	Frames	Payload_Bytes	PCR	TCP_Flags	Protoc	iRTT_ms	File_ID	Gantt_Chart
_d83...	2023-12-18 13:56:15	2023-12-18 13:56:36	00:00:21.1327380	461	272679	-1.00	AP SY	14.5	28.939	1	
_d83...	2023-12-18 13:56:15	2023-12-18 13:56:56	00:00:40.9032410	15	2960	-0.03	AP SY	27.3	28.484	1	
_d83...	2023-12-18 13:56:36	2023-12-18 13:57:17	00:00:40.9167590	23	7356	-0.72	AP SY	18.1	29.432	1	
_d83...	2023-12-18 13:56:56	2023-12-18 13:57:37	00:00:40.9281660	15	2960	-0.03	AP SY	25.1	28.496	1	
_d83...	2023-12-18 13:57:17	2023-12-18 13:57:58	00:00:40.8888160	17	3011	-0.34	AP SY	26.0	28.555	1	
_d83...	2023-12-18 13:57:37	2023-12-18 13:58:18	00:00:41.2518520	16	2966	-0.04	AP SY	25.2	37.365	1	
_d83...	2023-12-18 13:57:58	2023-12-18 13:58:40	00:00:42.2638010	25	8311	-0.75	AP SY	28.1	45.810	1	
_d83...	2023-12-18 13:58:18	2023-12-18 13:58:20	00:00:01.7315870	22	7922	-0.60	AP R	23.7	31.421	1	
_d83...	2023...										

Erik Hjelmvik

,

Thursday, 04 January 2024 10:12:00 (UTC/GMT)

In this video I analyze a pcap file with network traffic from Cobalt Strike Beacon using CapLoader.

The pcap file and Cobalt Strike malware config can be downloaded from Recorded Future's Triage sandbox.

Cobalt Strike Beacon configs can also be extracted locally with help of Didier Stevens' 1768.py or Fox-IT's dissect.cobaltstrike.

IOC List

- MD5 99516071d8f3e78e51200948bf377c4c
- SHA1 59fe505b24bdfa54ee6e4188ed8b88af9a42eb86
- SHA256 10e68f3e6c73161a1bba85ef9bada0cd79e25382ea8f8635bec4aa51bfe6c707
- JA3 a0e9f5d64349fb13191bc781f81f42e1
- JA4 t12d190800_d83cc789557e_7af1ed941c26
- IP:port 104.21.88.185:2096 (Cloudflare)

- Domain mail.googlesmail.xyz (Go Daddy)

Network Forensics Training

Are you interested in learning more about how to analyze network traffic from Cobalt Strike and other backdoors, malware and hacker tools? Then take a look at our upcoming network forensics classes!

Posted by Erik Hjelmvik on Thursday, 04 January 2024 10:12:00 (UTC/GMT)

Tags: #Cobalt Strike #CobaltStrike #Triage #JA3 #a0e9f5d64349fb13191bc781f81f42e1 #ThreatFox #CapLoader #Video #videotutorial

Recent Posts

» Hunting for Cobalt Strike in PCAP

» Network Forensics Training - Spring 2024

» CapLoader 1.9.6 Released

» Forensic Timeline of an IcedID Infection

» NetworkMiner 2.8.1 Released

Blog Archive

» 2024 Blog Posts

» 2023 Blog Posts

» 2022 Blog Posts

» 2021 Blog Posts

» 2020 Blog Posts

» 2019 Blog Posts

» 2018 Blog Posts

» 2017 Blog Posts

» 2016 Blog Posts

» 2015 Blog Posts

» 2014 Blog Posts

» 2013 Blog Posts

» 2012 Blog Posts

» 2011 Blog Posts

List all blog posts

Video blog posts

News Feeds

» Google News

» FeedBurner

» RSS Feed

NETRESEC on X / Twitter: @netresec

NETRESEC on Mastodon: @netresec@infosec.exchange